



A Professional Limited Liability Company

307 North Michigan Avenue, Suite 1020  
Chicago, Illinois 60601  
Telephone: 312-372-3930  
Facsimile: 312-372-3939

**Washington, D.C. Office**  
1333 New Hampshire Ave, NW, Fl 2  
Washington, DC 20036

**St. Louis Office**  
1714 Deer Tracks Trail, Ste 215  
St. Louis, MO 63131

**Adriana L. Kissel**  
Admitted in Illinois and Maryland

September 16, 2011

**Via Federal Express**

Tracking No.: 7975279927652

Marlene H. Dortch, Secretary  
Federal Communications Commission  
Office of the Secretary  
9300 East Hampton Drive  
Capitol Heights, MD 20743

Received & Inspected

SEP 19 2011

FCC Mail Room


**Re: ET Docket No. 04-295; Alabama Broadband, LLC ("ABB")/ Systems Security and Integrity ("SSI") Plan**

Dear Ms. Dortch:

On behalf of ABB, we submit an original and four copies of the company's SSI Plan to be filed in ET Docket No. 04-295. We also include an additional copy of the SSI Plan and ask that you date-stamp it and return it in the enclosed, postage-paid envelope.

Please contact me at (312) 372-3930 with any questions. Thank you.

Regards,



Adriana L. Kissel

**Enclosures**

cc: Tom Early, Alabama Broadband, LLC  
David Ward (via USPS, First-Class Mail)  
Senior Legal Advisor  
Policy Division  
Public Safety and Homeland Security Bureau  
445 12<sup>th</sup> Street, SW  
Washington, DC 20554

No. of Copies rec'd 0+4  
List ABCDE

SEP 19 2011

**ALABAMA BROADBAND, LLC ("ABB")  
SYSTEMS SECURITY AND INTEGRITY PLAN**

FCC Mail Room

The Communications Assistance for Law Enforcement Act ("CALEA") contains provisions limiting law enforcement's interception of communications and access to call-identifying information. CALEA requires telecommunications carriers to ensure that any interception of communications or access to call-identifying information that takes place on the carrier's premises be activated only in accordance with a court order or other lawful authorization, and that a selected carrier employee authorize the interception or access. CALEA applies to facilities-based broadband Internet access services and interconnected Voice over Internet Protocol ("VoIP") services.

This Plan sets out ABB's procedures and policies for complying with these CALEA requirements for its facilities-based broadband Internet access services.

**1. Definitions.**

**Appropriate legal authorization.** A court order signed by a judge or magistrate, or other authorization (such as a subpoena or warrant) pursuant to federal or state statute, authorizing the interception of an ABB customer's communications or access to call-identifying information. Examples of appropriate legal authorization are set forth on Exhibit 1.

**Appropriate carrier authorization.** Authorization by the CALEA Compliance Officer allowing personnel to enable law enforcement officials to intercept communications or access call-identifying information.

**Call-identifying information .** In the voice context, call-identifying information is the dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier. In the broadband context, call-identifying information is defined by industry standard-setting bodies and law enforcement agencies.

**Government.** The government or any agency of the United States, or any State or political subdivision authorized to conduct electronic surveillance—usually a federal or state law enforcement agency ("LEA").

**2. Interception of communications and access to call-identifying information.**

ABB personnel **shall not** permit government entities to intercept customer communications or to access call-identifying information without appropriate authorization. Appropriate authorization includes: (i) appropriate legal authorization; and (ii) the authorization of ABB's CALEA Compliance Officer.

Any such requests by a government entity must be immediately referred to Tom Early, ABB's CALEA Compliance Officer or, if unavailable, Reece Wallin, Director of MIS.

**3. Responsibilities of CALEA Compliance Officer.** The CALEA Compliance Officer shall determine if there is appropriate legal authorization for the interception of communications or access to call-identifying information.

- A. Appropriate legal authorization.** ABB's CALEA Compliance Officer shall not allow government entities to intercept communications or to access call-identifying information without appropriate legal authorization, as specified in Exhibit 1.

For requests other than those detailed in Exhibit 1, the CALEA Compliance Officer shall contact legal counsel to determine if appropriate legal authorization exists.

- B. Authorization form.** Where appropriate legal authorization exists, the CALEA Compliance Officer shall authorize appropriate personnel to intercept communications or provide call-identifying information on the Authorization and Certification Form attached as Exhibit 2.
- C. Emergency interception form.** Where a law enforcement officer requests an emergency interception, the CALEA Compliance Officer shall also complete the emergency interception form attached as Exhibit 3.
- D. Questions regarding legal authorization.** If unable to determine whether appropriate legal authorization exists, the CALEA Compliance Officer shall contact legal counsel for assistance.
- E. Report unauthorized acts.** The CALEA Compliance Officer shall report to affected law enforcement agencies, within a reasonable time, any unauthorized access to a lawful interception, or any act of unlawful electronic surveillance on ABB's premises, and shall fill out the Unauthorized Interception/Access /Surveillance Form attached as Exhibit 4.
- F. Maintain records of interceptions.** ABB's CALEA Compliance Officer shall be responsible for maintaining records of interceptions for a period of 5 years from the start date of the interception listed on the Authorization and Certification Form attached as Exhibit 2. The Form shall be completed within a reasonable period of time after the interception and shall include the following information:
- The IP address, telephone number, circuit number and/or account involved;
  - The start date and time that the carrier enables the interception;
  - The identity of the law enforcement officer presenting the authorization;
  - The name of the person signing the authorization;
  - The type of interception;
  - The name of the CALEA Compliance Officer;
  - The signature of the CALEA Compliance Officer, with a certification that the record is complete and accurate; and,
  - The legal authorization and any extensions that have been granted.

- G. **Maintain a copy of this Plan.** The CALEA Compliance Officer shall maintain a copy of this Plan and shall be familiar with these procedures.
- H. **Resubmission to the FCC.** If ABB (i) revises this Plan; (ii) merges with any other entity; or (iii) divests its interest in any other entity, the CALEA Compliance Officer shall resubmit this Plan to the FCC within 90 days of modification, merger, or divestiture.

**EXHIBIT 1**  
**Legal Authorization for Broadband-Related Information**

<b>Surveillance Requested</b>	<b>Minimum Authority Necessary for LEA Access</b>	<b>Exceptions where authority is not necessary</b>	<b>Limitations on authority</b>
<b>Pen register or trap and trace device (i.e., requests for source and destination information)</b>	<b>Court Order</b>  The order must specify: <ol style="list-style-type: none"> <li>1. The identity (if known) of the customer;</li> <li>2. The identity (if known) of the subject of the investigation;</li> <li>3. The IP address or other identifier, and the location where the device is to be attached;</li> <li>4. In the case of a state LEA, the geographic limits of the order;</li> <li>5. The offense to which the request relates.</li> </ol>	<ol style="list-style-type: none"> <li>1. Where the LEA reasonably determines that (A) an <b>emergency situation</b> exists involving (i) immediate danger or death or serious bodily injury; (ii) conspiratorial activities characteristic of organized crime; (iii) an immediate threat to national security; (iv) an ongoing attack on a protected computer; or (B) there are grounds for the issuance a court order, but the situation requires interception before one can be obtained.</li> <li>2. Where the customer consents.</li> </ol>	<ol style="list-style-type: none"> <li>1. The LEA must use technology reasonably available to restrict the recording or decoding to routing and addressing information (i.e., the contents of the transmission cannot be intercepted).</li> <li>2. The order cannot exceed 60 days (but the LEA can obtain extensions).</li> </ol>
<b>Interception of message content (for communication in transit)</b>	<b>Court Order</b>  The order must specify: <ol style="list-style-type: none"> <li>1. The identity (if known) of the customer;</li> <li>2. The facilities where authority to intercept is granted;</li> <li>3. The type of communication sought;</li> <li>4. The offense to which the interception relates;</li> <li>5. The identity of LEA;</li> <li>6. The judge or magistrate authorizing the interception;</li> <li>7. The period during which the interception is authorized, and whether or not the interception terminates when the communication is obtained.</li> </ol>	<ol style="list-style-type: none"> <li>1. Where the LEA reasonably determines that (A) an <b>emergency situation</b> exists involving (i) immediate danger or death or serious bodily injury; (ii) conspiratorial activities characteristic of organized crime; or (iii) conspiratorial activities threatening national security; and (B) there are grounds for the issuance a court order, but the situation requires interception before one can be obtained.</li> <li>2. Where one party to the communication consents.</li> </ol>	<ol style="list-style-type: none"> <li>1. The order cannot exceed 30 days (but the LEA can obtain extensions). The 30 day period begins on the earlier of the day the interception begins, or 10 days after the order is entered.</li> <li>2. In an emergency situation, the LEA must apply for an order within 48 hours.</li> </ol>
<b>Interception of contents of communication (for example,</b>	<b>Warrant</b>	<ol style="list-style-type: none"> <li>1. Where the originator or addressee consents to the disclosure.</li> </ol>	

Surveillance Requested	Minimum Authority Necessary for LEA Access	Exceptions where authority is not necessary	Limitations on authority
email) electronically stored for 180 days or fewer		<ol style="list-style-type: none"> <li>2. If the contents were (i) inadvertently obtained by ABB, and (ii) appear to pertain to the commission of a crime.</li> <li>3. If ABB believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	
Interception of contents of communication (for example, email) electronically stored for more than 180 days	<p><b>Warrant, or, if prior notice is given to the subscriber, a court order or administrative subpoena</b></p>	<ol style="list-style-type: none"> <li>1. Where the originator or addressee consents to the disclosure.</li> <li>2. If the contents were (i) inadvertently obtained by ABB, and (ii) appear to pertain to the commission of a crime.</li> <li>3. If ABB believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	
Basic customer information	<p><b>Administrative or trial subpoena, warrant, or court order</b></p> <p>Records that can be released include customer name, address, records of session times and durations, length of service, types of service, network address, and means and source of payment.</p> <p><b>Certification in writing from the Director of the FBI or his designee</b></p>	<ol style="list-style-type: none"> <li>1. Where the customer consents.</li> </ol>	<ol style="list-style-type: none"> <li>1. Limited to records showing name, address, length of service, and local or long distance toll billing.</li> <li>2. Records can be obtained only where relevant to an investigation to protect against international terrorism or clandestine intelligence activities.</li> </ol>

<b>Surveillance Requested</b>	<b>Minimum Authority Necessary for LEA Access</b>	<b>Exceptions where authority is not necessary</b>	<b>Limitations on authority</b>
<b>Other customer records related to internet services</b>	<b>Warrant or court order</b>	<ol style="list-style-type: none"> <li>1. Where the customer consents.</li> <li>2. If ABB believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.</li> </ol>	

## EXHIBIT 2

### AUTHORIZATION AND CERTIFICATION FORM

I certify that the attached law enforcement request for interception of (check appropriate box(es)):

- ☐ Interception of communications
- ☐ Access to call-identifying information

is based on both appropriate legal authorization and appropriate carrier authorization, as those terms are defined in Reservation Telephone Cooperative's Systems Security and Integrity Plan, and, based on these authorizations, the interception/access should be enabled.

ATTACH A COPY OF THE COURT ORDER OR OTHER WRITTEN AUTHORIZATION THAT IS THE BASIS OF LEGAL AUTHORIZATION. IF A COURT ORDER IS NOT USED, OR IF THE ORDER DOES NOT CONTAIN THE INFORMATION BELOW, COMPLETE THIS INFORMATION:

IP addresses, telephone numbers, circuit numbers, and/or accounts involved: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Start date and time of the interception: \_\_\_\_\_

Identity of law enforcement personnel: \_\_\_\_\_  
\_\_\_\_\_

Name of person authorizing interception/access: \_\_\_\_\_

Type of interception or access to call-identifying information: \_\_\_\_\_  
\_\_\_\_\_

I certify that the above information is complete and accurate to the best of my knowledge.

\_\_\_\_\_  
Signature of CALEA Compliance  
Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

**EXHIBIT 3**

**EMERGENCY INTERCEPTION FORM**

Name of Officer: \_\_\_\_\_

Badge or ID number: \_\_\_\_\_

Position: \_\_\_\_\_

Law Enforcement Agency: \_\_\_\_\_

Interception requested:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I certify that the above-referenced Officer has confirmed to me that an emergency situation exists that involves:

- (i) immediate danger of death or serious physical injury;
- (ii) conspiratorial activities threatening the national security interest;
- (iii) conspiratorial activities characteristic of organized crime; or
- (iv) an ongoing attack on a protected computer,

and that there are grounds upon which an order could be entered authorizing this interception, however, interception is required before an order could, with due diligence, be obtained.

\_\_\_\_\_  
Signature of CALEA Compliance Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

**EXHIBIT 4**  
**Unauthorized Acts**

**UNAUTHORIZED INTERCEPTION/ACCESS/SURVEILLANCE FORM**

The following incident occurred involving (check one)

☐ Unlawful interception of communications or access to call-identifying information

☐ Unlawful electronic surveillance on Reservation Telephone Cooperative's premises

[describe] \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
Signature of CALEA Compliance  
Officer

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

## **APPENDIX 1**

### **ABB's CALEA Compliance Officer: Tom Early**

ABB's CALEA Compliance Officer is responsible for ensuring that any interception of communications or access to call-identifying information that takes place ABB's premises be activated only in accordance with a court order or other lawful authorization. The CALEA Compliance Officer is also responsible for reporting any unauthorized surveillance or disclosures of call-identifying information to appropriate law enforcement personnel, and is responsible for maintaining records of any interceptions.

### **The CALEA Compliance Officer may be contacted at the following telephone numbers:**

Work Phone: (205) 426-3432

Cell Phone: (205) 789-3665

### **In the event that the CALEA Compliance Officer is unavailable, please contact:**

Name: Reece Wallin

Title: Director of MIS

Work Phone: (270) 333-3366

Cell Phone: (270) 997-0234